PA990594

ABSTRACT

Method and apparatus for encrypting transmission traffic at separate protocol layers L1, L2, and L3 so that separate encryption elements can be assigned to separate types of transmission traffic, which allows the implementation of different levels of encryption according to service requirements. Encryption elements use variable value inputs, called crypto-syncs, along with semi-permanent encryption keys to protect from replay attacks from rogue mobile stations. Since crypto-sync values vary, a method for synchronizing crypto-syncs at the mobile station and base station is also presented.